ABSTRACT

The present invention concerns a countermeasure method in an electronic component using a public key cryptography algorithm based on the use of elliptic curves. From a private key d and a number of points n on an elliptic curve, a new deciphering integer d′ is calculated. The present invention applies particularly to any existing electronic component, such as a smart card.